RESOURCE CENTER

Informe sobre el estado de la seguridad de las contraseñas 2024

Cómo abordan los organismos federales la seguridad de las contraseñas

Get the full interactive view at
https://bitwarden.com/es-la/resources/the-state-of-password-security/

bitwarden

Evaluación del estado de la seguridad de las contraseñas en las agencias federales de EE.UU.

En los últimos años, el Gobierno Federal de los Estados Unidos se ha centrado intensamente en la ciberseguridad, y muchos organismos han tomado la iniciativa en la educación de las organizaciones gubernamentales y las empresas grandes y pequeñas, así como de los consumidores.

Sin embargo, cuando se trata de la seguridad de las contraseñas, no todas las agencias cantan la misma melodía. Uno de los grupos más destacados, el Instituto Nacional de Normas y Tecnología (NIST), "desarrolla normas de ciberseguridad, directrices, mejores prácticas y otros recursos para satisfacer las necesidades de la industria estadounidense, las agencias federales y el público en general".

La página de ciberseguridad del NIST continúa diciendo que "algunas tareas de ciberseguridad del NIST están definidas por estatutos, órdenes ejecutivas y políticas federales. Por ejemplo, la Oficina de Gestión y Presupuesto (OMB) ordena que todos los organismos federales apliquen las normas y orientaciones de ciberseguridad del NIST para los sistemas de seguridad no nacionales".

Por desgracia, las recomendaciones del NIST aún no han sido universalmente aceptadas y aplicadas por todos los organismos federales. Y aunque el NIST establece las normas que las agencias pretenden seguir, incluso tiene su propia debilidad en forma de sitio web desorganizado.

2024 es el tercer año que Bitwarden realiza este análisis. A lo largo de tres años, el sitio web del NIST ha permanecido desorganizado, aunque su contenido es muy sólido. También se han producido algunos avances positivos. La Casa Blanca ha mejorado la difusión de consejos sobre seguridad de contraseñas, pasando de una calificación de "Mejorable" a "Buena". Otros organismos que han mejorado sus recomendaciones de seguridad de contraseñas y su postura general en materia de ciberseguridad son la Asociación de Ciberseguridad y Seguridad de Infraestructuras (CISA), la Oficina Federal de Investigación (FBI), la Comisión Federal de Comercio (FTC) y la Administración de Pequeñas Empresas (SBA).

Este año, Bitwarden también ha añadido la Comisión del Mercado de Valores (SEC) a este informe. El año pasado, la SEC adoptó normas que obligan a las empresas a revelar los incidentes importantes de ciberseguridad. Dado el papel de la SEC en la aplicación del cumplimiento de la ciberseguridad, este informe evaluará el propio asesoramiento de la SEC en materia de seguridad de contraseñas.

La tecnología avanza deprisa. Para las empresas y los particulares, gran parte de nuestras vidas están ahora en línea, en una miríada de cuentas que van desde divertidos sitios de entretenimiento a serios asuntos financieros, como nuestras cuentas bancarias.

El objetivo de esta evaluación es involucrar y educar a todos los que utilizan contraseñas sobre las mejores prácticas procedentes del gobierno federal y dónde hay margen de mejora. Hay muchos dentro del gobierno federal que tienen un sólido enfoque educativo sobre la seguridad de las contraseñas, y hay otros que podrían necesitar un poco de ayuda para modernizarse.

Afortunadamente, se está creando un consenso sobre las mejores prácticas para la seguridad de las contraseñas. Este informe consolida y evalúa los detalles.

The State of Password Security: How federal agencies are addressing password security

Download

Ver la Presentación sobre el estado de la seguridad de las contraseñas

Índice

Pautas para el sistema de clasificación de seguridad de contraseñas

El sistema de calificación clasifica a las agencias en función del cumplimiento de los siguientes criterios:

Excellent

- Recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- El asesoramiento general sobre seguridad está actualizado y cumple las directrices del NIST
- Expone las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Very Good

- Recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- El asesoramiento general sobre seguridad está actualizado y cumple las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Good

- No recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Fair

- No recomienda el uso de un gestor de contraseñas

- Recuerda la importancia de las contraseñas seguras
- No menciona sistemáticamente la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas.
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Room for Improvement

- No recomienda el uso de un gestor de contraseñas
- No destaca la importancia de contraseñas seguras
- No menciona la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas.
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Instituto Nacional de Normas y Tecnología (NIST)

Marco de gestión de riesgos del NIST | IA-5(18)

Consejo de la Agencia:

- Gestión de autenticadores | Gestores de contraseñas
  - Emplear [Asignación: Gestores de contraseñas definidos por la organización] para generar y gestionar contraseñas; y
    - Proteja las contraseñas mediante [asignación: controles definidos por la organización].
    - En los sistemas en los que se utilizan contraseñas estáticas, a menudo es difícil garantizar que las contraseñas sean lo suficientemente complejas y que no se utilicen las mismas contraseñas en varios sistemas. Un gestor de contraseñas es una solución a este problema, ya que genera y almacena automáticamente contraseñas seguras y diferentes para varias cuentas. Un riesgo potencial del uso de gestores de contraseñas es que los adversarios pueden apuntar a la colección de contraseñas generadas por el gestor de contraseñas. Por lo tanto, la recopilación de contraseñas requiere una protección que incluya el cifrado de las contraseñas y el almacenamiento de la recopilación fuera de línea en un token.

- Referencia

Directrices sobre identidad digital

Consejo de la Agencia:

- Los secretos memorizados DEBERÁN tener al menos 8 caracteres de longitud si los elige el abonado. Los secretos memorizados elegidos aleatoriamente por el CSP o el verificador DEBERÁN tener una longitud mínima de 6 caracteres y PODRÁN ser totalmente numéricos. Si el CSP o el verificador desautoriza un secreto memorizado elegido basándose en su aparición en una lista negra de valores comprometidos, SE EXIGIRÁ al abonado que elija un secreto memorizado diferente. No se DEBERÍA imponer ningún otro requisito de complejidad para los secretos memorizados. En el Apéndice A, Resistencia de los secretos memorizados, se presenta una justificación para ello.

- Los verificadores EXIGIRÁN que los secretos memorizados elegidos por el suscriptor tengan una longitud mínima de 8 caracteres. Los verificadores DEBERÍAN permitir secretos memorizados elegidos por el suscriptor de al menos 64 caracteres de longitud. Todos los caracteres de impresión ASCII [RFC 20] así como el carácter de espacio DEBERÍAN ser aceptables en secretos memorizados. También DEBERÍAN aceptarse caracteres Unicode [ISO/ISC 10646]. Para tener en cuenta posibles errores de escritura, los verificadores PUEDEN sustituir varios caracteres de espacio consecutivos por un único carácter de espacio antes de la verificación, siempre que el resultado tenga al menos 8 caracteres de longitud. NO SE DEBE truncar el secreto. A efectos de los requisitos de longitud anteriores, cada punto de código Unicode SE CONTARÁ como un único carácter.

- Los secretos memorizados elegidos aleatoriamente por el CSP (p. ej., en el momento de la inscripción) o por el verificador (p. ej., cuando un usuario solicita un nuevo PIN) SERÁN de al menos 6 caracteres de longitud y SE GENERARÁN utilizando un generador de bits aleatorios aprobado [SP 800-90Ar1].

- Los verificadores de secretos memorizados NO PERMITIRÁN al suscriptor almacenar una "pista" que sea accesible a un solicitante no autenticado. Los verificadores NO PEDIRÁN a los abonados que utilicen tipos específicos de información (por ejemplo, "¿Cómo se llamaba su primera mascota?") cuando elijan secretos memorizados.

- Al procesar solicitudes para establecer y cambiar secretos memorizados, los verificadores COMPARARÁN los posibles secretos con una lista que contenga valores conocidos por ser de uso común, esperados o comprometidos. Por ejemplo, la lista PUEDE incluir, entre otros, los siguientes elementos:
  - Contraseñas obtenidas de corpus de infracciones anteriores.
  - Palabras del diccionario.
  - Caracteres repetitivos o secuenciales (por ejemplo, "aaaaaa", "1234abcd").
  - Palabras específicas del contexto, como el nombre del servicio, el nombre de usuario y sus derivados.

- Si el secreto elegido se encuentra en la lista, el CSP o el verificador AVISARÁ al abonado de que tiene que seleccionar un secreto diferente, le indicará el motivo del rechazo y le pedirá que elija un valor distinto.

- Los verificadores DEBERÍAN ofrecer una guía al suscriptor, como un medidor de fuerza de contraseña [Meters], para ayudar al usuario a elegir un secreto memorizado fuerte. Esto es particularmente importante tras el rechazo de un secreto memorizado en la lista anterior, ya que desalienta la modificación trivial de los secretos memorizados de la lista (y probablemente muy débiles) [Listas negras].

- Los verificadores APLICARÁN un mecanismo de limitación de velocidad que limite efectivamente el número de intentos de autenticación fallidos que pueden realizarse en la cuenta del abonado, tal como se describe en la sección 5.2.2.

- Los verificadores NO DEBERÍAN imponer otras reglas de composición (por ejemplo, requerir mezclas de diferentes tipos de caracteres o prohibir caracteres repetidos consecutivamente) para los secretos memorizados. Los verificadores NO DEBERÍAN requerir que los secretos memorizados sean cambiados arbitrariamente (por ejemplo, periódicamente). Sin embargo, los verificadores DEBERÁN forzar un cambio si existen pruebas de que el autenticador está en peligro.

- Los verificadores DEBERÍAN permitir a los reclamantes utilizar la función "pegar" al introducir un secreto memorizado. Esto facilita el uso de gestores de contraseñas, que son muy utilizados y en muchos casos aumentan la probabilidad de que los usuarios elijan secretos memorizados más fuertes.

- Para ayudar al demandante a introducir con éxito un secreto memorizado, el verificador DEBERÍA ofrecer una opción para mostrar el secreto -en lugar de una serie de puntos o asteriscos- hasta que se introduzca. Esto permite al solicitante verificar su entrada si se encuentra en un lugar en el que es poco probable que se observe su pantalla. El verificador PUEDE también permitir que el dispositivo del usuario muestre los caracteres introducidos individualmente durante un breve espacio de tiempo después de teclear cada carácter para verificar que se ha introducido correctamente. Esto es especialmente aplicable a los dispositivos móviles.

- El verificador UTILIZARÁ un cifrado aprobado y un canal protegido autenticado cuando solicite secretos memorizados con el fin de proporcionar resistencia a las escuchas y a los ataques MitM.

- Los verificadores ALMACENARÁN los secretos memorizados de forma que sean resistentes a los ataques fuera de línea. Los secretos memorizados ESTARÁN salados y cifrados mediante una función adecuada de derivación de clave unidireccional. Las funciones de derivación de claves toman una contraseña, una sal y un factor de coste como entradas y luego generan un hash de la contraseña. Su objetivo es hacer que cada intento de adivinar la contraseña por parte de un atacante que haya obtenido un archivo hash de contraseñas sea costoso y, por lo tanto, que el coste de un ataque de adivinación sea alto o prohibitivo. Algunos ejemplos de funciones de derivación de claves adecuadas son Password-based Key Derivation Function 2 (PBKDF2) [SP 800-132] y Balloon [BALLOON]. Una función de memoria dura DEBERÍA utilizarse porque aumenta el coste de un ataque. La función de derivación de claves UTILIZARÁ una función unidireccional aprobada, como Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1], cualquier función hash aprobada en SP 800-107, Secure Hash Algorithm 3 (SHA-3) [FIPS 202], CMAC [SP 800-38B] o Keccak Message Authentication Code (KMAC), Customizable SHAKE (cSHAKE), o ParallelHash [SP 800-185]. La longitud de salida elegida de la función de derivación de claves DEBERÍA ser la misma que la longitud de salida de la función unidireccional subyacente.

- La sal SERÁ de al menos 32 bits de longitud y se elegirá arbitrariamente para minimizar las colisiones de valores de sal entre los hashes almacenados. Tanto el valor de la sal como el hash resultante SE ALMACENARÁN para cada abonado utilizando un autenticador secreto memorizado.

- Para PBKDF2, el factor de coste es un recuento de iteraciones: cuantas más veces se itere la función PBKDF2, más tiempo se tarda en calcular el hash de la contraseña. Por lo tanto, el recuento de iteraciones DEBERÍA ser tan grande como lo permita el rendimiento del servidor de verificación, normalmente al menos 10.000 iteraciones.

- Además, los verificadores DEBERÍAN realizar una iteración adicional de una función de derivación de claves utilizando un valor de sal que sea secreto y conocido sólo por el verificador. Este valor de sal, si se utiliza, SERÁ generado por un generador de bits aleatorios aprobado [SP 800-90Ar1] y proporcionará al menos la fuerza de seguridad mínima especificada en la última revisión de SP 800-131A (112 bits a partir de la fecha de esta publicación). El valor secreto de la sal SE ALMACENARÁ por separado de los secretos memorizados con hash (por ejemplo, en un dispositivo especializado como un módulo de seguridad de hardware). Con esta iteración adicional, los ataques de fuerza bruta a los secretos memorizados con hash son impracticables mientras el valor secreto de la sal siga siendo secreto.

- Serie de blogs del Mes de concienciación sobre la ciberseguridad 2023
  - Asesoramiento de la Agencia
    - Las contraseñas siguen siendo el mecanismo de autenticación más utilizado para acceder a los recursos de interés. Las contraseñas son la primera línea de defensa para proteger la confidencialidad e integridad de los datos contra los ciberdelincuentes y las violaciones de datos. Unas contraseñas buenas y seguras ayudan a las personas a mantenerse seguras y privadas en Internet.

- Referencia

NIST

bitwarden

Instituto Nacional de Normas y Tecnología (NIST)

Valoración global de Bitwarden: Muy buena

- Recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- El asesoramiento general en materia de seguridad está actualizado y cumple las directrices del NIST (el NIST establece la norma para el asesoramiento en materia de seguridad del Gobierno federal).
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

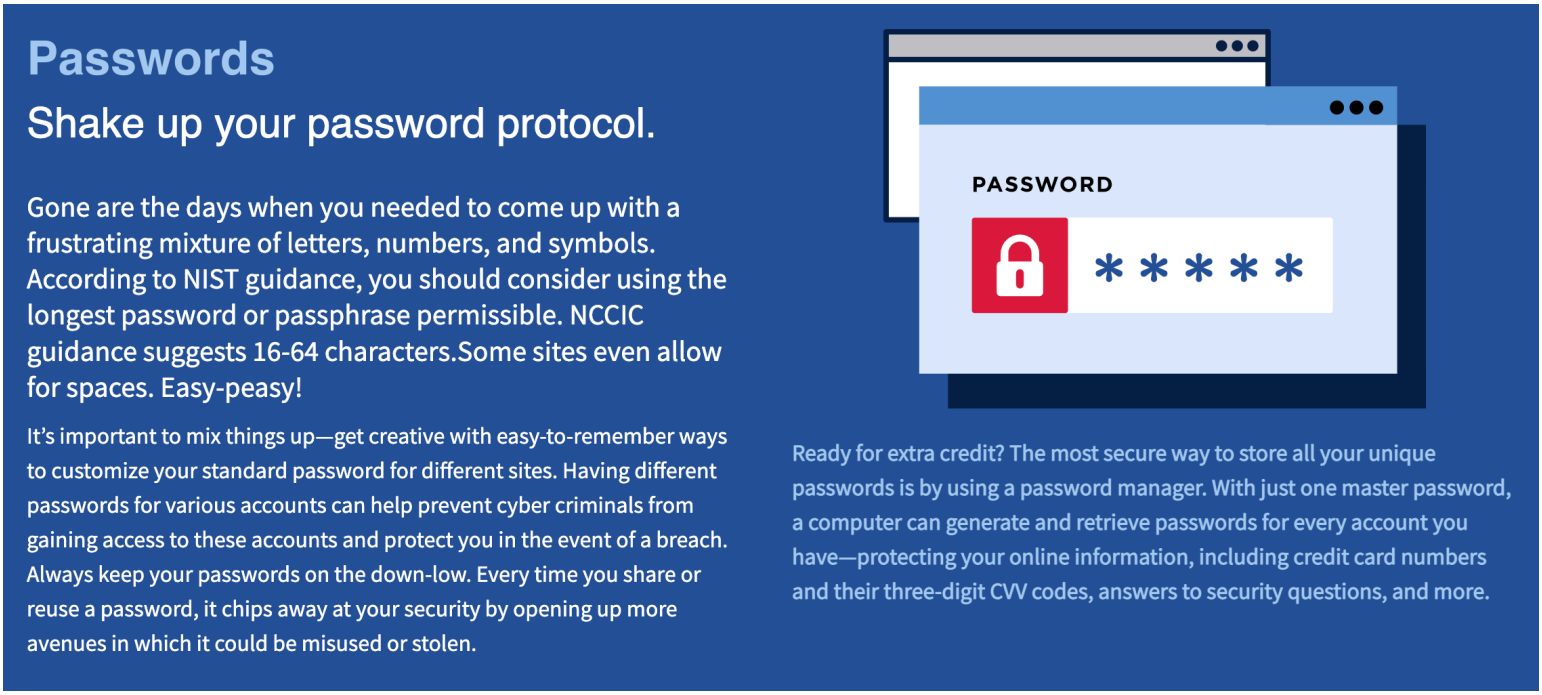
Aunque el asesoramiento es exhaustivo y establece las normas para las agencias, el acceso a las directrices sobre contraseñas a través del sitio web no es intuitivo. Los consejos están enterrados en PDF muy largos y redactados de una manera que no es fácil de usar.

"Verifiers SHOULD permit claimants to use “paste” functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets."

NIST

Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA)

Ciberlecciones



Lecciones cibernéticas sobre contraseñas, CISA

- Referencia

Guía Stop Ransomware

Consejo de la Agencia:

- Implantar políticas de contraseñas que exijan contraseñas únicas de al menos 15 caracteres.
  - Los gestores de contraseñas pueden ayudarte a desarrollar y gestionar contraseñas seguras. Asegure y limite el acceso a cualquier gestor de contraseñas en uso y active todas las funciones de seguridad disponibles en el producto en uso, como MFA.

- Referencia

Asegure nuestro mundo: Exigir contraseñas seguras

Consejo de la Agencia:

- Las pequeñas y medianas empresas son un objetivo habitual de los piratas informáticos malintencionados y un punto de entrada habitual para los ladrones digitales son las contraseñas robadas o débiles.

- Pero la buena noticia es que puede mantener su empresa segura exigiendo a los empleados que utilicen contraseñas seguras y gestores de contraseñas.

- Dé ejemplo utilizando contraseñas largas, aleatorias y únicas en todas sus cuentas personales y profesionales, y utilice un gestor de contraseñas para recordarlas. A continuación, trabaje con su personal o proveedor de TI para exigir a los empleados que utilicen contraseñas seguras para acceder a sus sistemas. Así mantendrás tus datos seguros y protegidos.

- Referencia

Asegurar nuestro mundo: Contraseñas débiles

Consejo de la Agencia:

- Deja que un gestor de contraseñas haga el trabajo Un gestor de contraseñas crea, almacena y rellena las contraseñas por nosotros de forma automática. Así, cada uno de nosotros sólo tendrá que recordar una contraseña segura para el propio gestor de contraseñas. Busca "gestores de contraseñas" en fuentes de confianza, como Consumer Reports, que ofrece una selección de gestores de contraseñas muy bien valorados. Lee los comentarios para comparar opciones y encontrar un programa de confianza para ti.

- Referencia

bitwarden

Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA)

Valoración global de Bitwarden: Muy buena

- Recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- El asesoramiento general sobre seguridad está actualizado y cumple las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

La Agencia de Seguridad Nacional (NSA)

Guía Stop Ransomware

Consejo de la Agencia:

- Implantar políticas de contraseñas que exijan contraseñas únicas de al menos 15 caracteres.
  - Los gestores de contraseñas pueden ayudarte a desarrollar y gestionar contraseñas seguras. Asegure y limite el acceso a cualquier gestor de contraseñas en uso y active todas las funciones de seguridad disponibles en el producto en uso, como MFA.
- Referencia

Tipos de contraseña Cisco: Mejores prácticas

Consejo de la Agencia:

- El aumento del número de ataques a infraestructuras de red en los últimos años nos recuerda que la autenticación de los dispositivos de red es una consideración importante. Los dispositivos de red podrían verse comprometidos debido a:
  - Mala elección de la contraseña (vulnerable a la fuerza bruta)
  - Archivos de configuración del router (que contienen contraseñas cifradas) enviados por correo electrónico sin cifrar, o
  - Contraseñas reutilizadas (cuando las contraseñas recuperadas de un dispositivo comprometido pueden utilizarse para comprometer otros dispositivos).
- El uso de contraseñas por sí solas aumenta el riesgo de explotación del dispositivo. Aunque la NSA recomienda encarecidamente la autenticación multifactor para los administradores que gestionan dispositivos críticos, a veces es necesario utilizar únicamente contraseñas. Elegir buenos algoritmos de almacenamiento de contraseñas puede dificultar mucho la explotación.
- Para ofrecer la máxima protección posible, utilice contraseñas seguras para evitar que puedan ser descifradas y convertidas en texto plano. Cumplir con una política de contraseñas que:
  - Consiste en una combinación de letras minúsculas y mayúsculas, símbolos y números;
  - Tiene al menos 15 caracteres alfanuméricos; y

- Patrones que no lo son:
  - Un paseo por el teclado
  - Lo mismo que un nombre de usuario
  - La contraseña por defecto
  - Igual que una contraseña utilizada en cualquier otro lugar
  - Relacionados con la red, la organización, la ubicación u otros identificadores de función
  - Directamente del diccionario, acrónimos comunes o fáciles de adivinar
- Referencia

Seguridad en las redes sociales

Consejo de la Agencia:

- Proteja y refuerce sus contraseñas
  - Utilice contraseñas únicas y seguras para cada cuenta en línea. La reutilización de contraseñas en varias cuentas puede exponer los datos de todas las cuentas si se descubre la contraseña. Asegúrese de que su contraseña tiene la longitud y complejidad adecuadas, utilizando una combinación de letras, números y caracteres especiales. Siempre que sea posible, aplica la autenticación multifactor mediante un token o una aplicación de autenticación para que nadie pueda acceder a tu cuenta aunque tu contraseña esté en peligro. No comparta nunca contraseñas y evite utilizar información que pueda adivinarse a partir de sus perfiles en redes sociales o información pública.
- Referencia

Selección de soluciones seguras de autenticación multifactor

Consejo de la Agencia:

- Los mecanismos de autenticación multifactor de respuesta única requieren la activación del dispositivo, ya sea con un PIN/contraseña o biométrico. El dispositivo proporciona "lo que tienes" y su activación implica que "lo que sabes" o "lo que eres" ha sido verificado.
- Por otro lado, los autenticadores de varios pasos suelen incluir una contraseña para proporcionar "lo que sabes" y otro autenticador que proporciona "lo que tienes". Las agencias gubernamentales de EE.UU. deben considerar los requisitos para la activación de PIN/contraseña, así como para las contraseñas que se utilizan directamente para proporcionar "lo que se sabe". Las directrices de SP 800-63-3 Parte B indican que los secretos memorizados (tanto para la activación como para el autenticador de factor único) deben tener al menos entre 6 y 8 caracteres, y recomienda una mayor fortaleza de la contraseña para las contraseñas seleccionadas por el usuario. A la hora de determinar los requisitos de las contraseñas, tenga en cuenta que los dispositivos multifactor deben integrar umbrales estrictos para hacer frente a los ataques de adivinación de contraseñas, mientras que los verificadores podrían emplear mecanismos de umbral menos estrictos que garanticen que las contraseñas que se utilizan directamente tengan requisitos de mayor fortaleza.
- Referencia

Very Good

bitwarden

La Agencia de Seguridad Nacional (NSA)

Valoración global de Bitwarden: Buena

- No recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- Los consejos generales de seguridad no están actualizados ni se ajustan a las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

"Disable the feature that allows web browsers to remember your passwords. Secure your passwords in a password manager."

NSA

Departamento de Seguridad Interior

La CISA depende del DHS

Página sobre ciberseguridad

Consejo de la Agencia:

- El Presidente Biden ha hecho de la ciberseguridad, un elemento crítico de la misión del Departamento de Seguridad Nacional (DHS), una de las principales prioridades de la Administración Biden-Harris a todos los niveles de gobierno.
- Para avanzar en el compromiso del Presidente, y para reflejar que la mejora de la resistencia de la ciberseguridad de la nación es una prioridad máxima para el DHS, el Secretario Mayorkas hizo un llamamiento a la acción dedicado a la ciberseguridad en su primer mes en el cargo. Este llamamiento a la acción se centró en hacer frente a la amenaza inmediata del ransomware y en crear una plantilla más sólida y diversa.
- En marzo de 2021, el Secretario Mayorkas esbozó su visión más amplia y una hoja de ruta para los esfuerzos de ciberseguridad del Departamento en un discurso virtual organizado por la Conferencia RSA, en colaboración con la Universidad de Hampton y las Girl Scouts of the USA.
- Tras su presentación, el Secretario se reunió con Judith Batty, Directora General interina de las Girls Scouts, en una charla informal para hablar de los retos de ciberseguridad sin precedentes a los que se enfrenta actualmente Estados Unidos. La Dra. Chutima Boonthum-Denecke, del Departamento de Informática de la Universidad de Hampton, presentó al Secretario y facilitó un turno de preguntas y respuestas para clausurar el programa.
  - Visión general de los sprints de ciberseguridad del DHS

Departamento de Seguridad Interior

Valoración global de Bitwarden: Mejorable

- No recomienda el uso de un gestor de contraseñas
- No destaca la importancia de contraseñas seguras
  - Ofrece consejos inexactos y erróneos sobre la seguridad de las contraseñas O no menciona las contraseñas ni su seguridad
  - No indica claramente los consejos relacionados con las contraseñas
- No menciona sistemáticamente la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas.
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Oficina Federal de Investigación (FBI)

La ciberamenaza

Consejo de la Agencia:

- Los delitos e intrusiones cibernéticas a través de Internet son cada vez más sofisticados y prevenirlos requiere que cada usuario de un dispositivo conectado esté atento y en guardia.
- Mantenga los sistemas y el software actualizados e instale un programa antivirus potente y de confianza.
- Tenga cuidado al conectarse a una red Wi-Fi pública y no realice ninguna transacción sensible, incluidas compras, cuando esté en una red pública.
- Crea una contraseña fuerte y única para cada cuenta en línea y cámbiala con regularidad.
- Configura la autenticación multifactor en todas las cuentas que lo permitan.
- Examine la dirección de correo electrónico en toda la correspondencia y las URL de los sitios web antes de responder a un mensaje o visitar un sitio.
- No haga clic en mensajes de correo electrónico o de texto no solicitados.
- Tenga cuidado con la información que comparte en perfiles en línea y cuentas de redes sociales. Compartir cosas como nombres de mascotas, escuelas y miembros de la familia puede dar a los estafadores las pistas que necesitan para adivinar tus contraseñas o las respuestas a las preguntas de seguridad de tu cuenta.
- No envíe pagos a personas u organizaciones desconocidas que busquen ayuda monetaria e inste a actuar de inmediato.
- Referencia

Estafas y seguridad en Internet

Consejo de la Agencia:

- **Mantenga activado el cortafuegos**

  Un cortafuegos ayuda a proteger el ordenador de piratas informáticos que podrían intentar acceder a él para bloquearlo, borrar información o incluso robar contraseñas u otra información confidencial. Los cortafuegos de software se recomiendan ampliamente para ordenadores individuales. El software está preempaquetado en algunos sistemas operativos o puede adquirirse para ordenadores individuales. En el caso de varios ordenadores conectados en red, los routers de hardware suelen proporcionar protección de cortafuegos.

- **Instale o actualice su software antivirus**

  El software antivirus está diseñado para evitar que programas maliciosos se incrusten en su ordenador. Si detecta código malicioso, como un virus o un gusano, trabaja para desactivarlo o eliminarlo. Los virus pueden infectar ordenadores sin que los usuarios lo sepan. La mayoría de los tipos de software antivirus pueden configurarse para que se actualicen automáticamente.

- **Instale o actualice su tecnología antispyware**

  Los programas espía son exactamente lo que parecen: programas que se instalan subrepticiamente en su ordenador para que otros puedan espiar sus actividades en él. Algunos programas espía recopilan información sobre usted sin su consentimiento o producen anuncios emergentes no deseados en su navegador web. Algunos sistemas operativos ofrecen protección gratuita contra programas espía, y en Internet o en la tienda de informática local se pueden descargar programas de bajo coste. Desconfíe de los anuncios en Internet que ofrecen programas antiespía descargables: en algunos casos, estos productos pueden ser falsos y contener en realidad programas espía u otros códigos maliciosos. Es como hacer la compra: compra donde confíes.

- **Mantenga actualizado su sistema operativo**

  Los sistemas operativos de los ordenadores se actualizan periódicamente para mantenerse en sintonía con los requisitos tecnológicos y corregir agujeros de seguridad. Asegúrese de instalar las actualizaciones para que su ordenador disponga de la protección más reciente.

- **Cuidado con lo que descarga**

  La descarga descuidada de archivos adjuntos de correo electrónico puede burlar incluso el software antivirus más vigilante. No abra nunca un archivo adjunto de correo electrónico de alguien que no conozca, y desconfíe de los archivos adjuntos reenviados por personas que sí conozca. Es posible que, sin saberlo, hayan hecho avanzar un código malicioso.

- **Apague el ordenador**

  Con el crecimiento de las conexiones a Internet de alta velocidad, muchos optan por dejar sus ordenadores encendidos y listos para la acción. El inconveniente es que estar "siempre encendido" hace que los ordenadores sean más susceptibles. Además de la protección mediante cortafuegos, diseñada para evitar ataques no deseados, al apagar el ordenador se interrumpe la conexión de un atacante, ya sea un programa espía o una red de bots que utiliza los recursos del ordenador para llegar a otros usuarios involuntarios.

- Referencia

Good

bitwarden

Oficina Federal de Investigación (FBI)

Valoración global de Bitwarden: Buena

- No recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Cita la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

"Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions."

FBI

Comisión Federal de Comercio (FTC)

Creación de contraseñas seguras y otras formas de proteger sus cuentas

Consejo de la Agencia:

- Otra opción es utilizar un gestor de contraseñas externo para crear una contraseña segura y recordarla. Para encontrar un gestor de contraseñas de confianza, lee las opiniones de los expertos. Asegúrate de que la contraseña que utilizas con el gestor de contraseñas es fuerte y segura. Un navegador web, un navegador móvil y un gestor de contraseñas pueden guardar tus contraseñas.
- Una contraseña segura es un primer paso importante para proteger su cuenta de los piratas informáticos. Pero incluso las contraseñas más seguras son vulnerables a los ciberataques. Utilizar la autenticación multifactor significa que un hacker que robe tu contraseña no podrá acceder a tu cuenta sin otro factor de autenticación.
- El tipo más común de autenticación multifactor es un código de verificación que recibes por mensaje de texto o correo electrónico. Esta contraseña de un solo uso suele tener seis dígitos o más y caduca automáticamente. Pero este es el tipo menos seguro de autenticación de dos factores, así que elige un método más seguro como una aplicación de autenticación o una clave de seguridad para una mayor protección, si tienes la opción.
- Referencia

Lista de control de contraseñas

Consejo de la Agencia:

- **Asegúrate de que tu contraseña es larga y segura.** Es decir, al menos 12 caracteres. Alargar una contraseña suele ser la forma más sencilla de hacerla más segura. Considere la posibilidad de utilizar una frase de contraseña de palabras aleatorias para que su contraseña sea más fácil de recordar, pero evite utilizar palabras o frases comunes. Si el servicio que utilizas no permite contraseñas largas, puedes reforzar tu contraseña mezclando letras mayúsculas y minúsculas, números y símbolos.

- **No reutilices contraseñas que hayas usado en otras cuentas.** Utilice contraseñas diferentes para las distintas cuentas. De este modo, si un pirata informático consigue tu contraseña para una cuenta, no podrá utilizarla para acceder a tus otras cuentas.

- **Utilice la autenticación multifactor cuando sea una opción.** Algunas cuentas ofrecen seguridad adicional al requerir algo más que una contraseña para acceder a ella. Esto se denomina autenticación multifactor. El "algo extra" que necesitas para acceder a tu cuenta se divide en dos categorías:
  - Algo que tienes, como un código de acceso que obtienes a través de una aplicación de autenticación o una clave de seguridad.
  - Algo que tú eres, como un escáner de tu huella dactilar, tu retina o tu cara.

- **Piensa en un gestor de contraseñas.** La mayoría de la gente tiene problemas para hacer un seguimiento de todas sus contraseñas. Cuanto más larga y complicada sea una contraseña, más segura será, pero una contraseña más larga también puede ser más difícil de recordar. Considere la posibilidad de almacenar sus contraseñas y preguntas de seguridad en un gestor de contraseñas de confianza. Para encontrar un gestor de contraseñas de confianza, busca en sitios de reseñas independientes y habla con amigos y familiares para saber cuáles utilizan. Asegúrate de utilizar una contraseña segura para proteger la información de tu gestor de contraseñas.

- **Elige preguntas de seguridad de las que sólo tú conozcas la respuesta.** Si un sitio le pide que responda a preguntas de seguridad, evite dar respuestas que estén disponibles en registros públicos o sean fáciles de encontrar en Internet, como su código postal, lugar de nacimiento o el apellido de soltera de su madre. Y no utilice preguntas con un número limitado de respuestas que los atacantes puedan adivinar fácilmente, como el color de su primer coche. Puedes incluso utilizar respuestas sin sentido para dificultar la adivinación, pero si lo haces, asegúrate de que puedes recordar las que utilices.

- **Cambie las contraseñas rápidamente si se produce una brecha.** Si una empresa le informa de que se ha producido una filtración de datos por la que un pirata informático podría haber obtenido su contraseña, cambie inmediatamente la contraseña que utiliza con esa empresa y en cualquier cuenta que utilice una contraseña similar.

- Referencia

Excellent

bitwarden

Comisión Federal de Comercio (FTC)

Valoración global de Bitwarden: Excelente

- Recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- El asesoramiento general sobre seguridad está actualizado y cumple las directrices del NIST
- Expone las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

"Use a password manager. A third-party password manager also can create a strong password. To find a reputable password manager, read expert reviews. Make sure the password for your password manager is strong. And protect it like you do your other passwords."

FTC

Departamento de Comercio

Mes Nacional de la Ciberseguridad: Protegerse en Internet

Consejo de la Agencia:

- Antes, lo habitual era crear contraseñas con caracteres especiales, mayúsculas, números, letras y una serie de reglas arbitrarias, como obligarte a cambiar tu contraseña varias veces al año. Los estudios demuestran que todos hemos reaccionado de la misma manera: hemos utilizado contraseñas o creado variaciones de la misma contraseña porque se nos había pedido que memorizáramos docenas de contraseñas únicas para cada sitio, inicio de sesión o aplicación.

- Nuestros instintos naturales crearon un punto débil en nuestra seguridad en línea y los ciberdelincuentes se aprovecharon de ello. La investigación sobre el uso de contraseñas ha demostrado la debilidad inherente a esperar que los usuarios memoricen contraseñas arbitrariamente complejas, y la importancia de utilizar la autenticación multifactor (AMF) para salvaguardar nuestra información privada. Lo importante es que nuestra forma de pensar ha evolucionado en torno a este tema, y hemos identificado las siguientes prácticas para protegernos mejor:
  - Cuando tenga que utilizar una contraseña, utilice una contraseña más larga (15 caracteres o más) o incluso frases de contraseña, ya que proporcionan una mayor protección que una contraseña más corta y arbitrariamente compleja. Las frases de contraseña tienen la ventaja añadida de ser fáciles de recordar.

  - El uso de MFA (como un código de un solo uso que se envía por correo electrónico o una aplicación de autenticación en el teléfono) añade una segunda capa fundamental para protegerse de una contraseña comprometida. La AMF debe configurarse siempre que esté disponible. Sólo te llevará un par de instantes y te dará tranquilidad.

- Los gestores de contraseñas, protegidos por una contraseña muy fuerte y larga con MFA activado, nos permiten crear contraseñas únicas para cada sitio sin necesidad de memorizarlas todas.

- Referencia

El NIST depende del Departamento de Comercio

Consejos de la Agencia:

- Garantizar la seguridad de nuestras redes mundiales interconectadas y de los dispositivos y datos conectados a ellas es uno de los retos que definen nuestra era.

- El Departamento de Comercio se encarga de mejorar la concienciación y las protecciones en materia de ciberseguridad, proteger la privacidad, mantener la seguridad pública, apoyar la seguridad económica y nacional y capacitar a los estadounidenses para gestionar mejor su seguridad en línea.
  - El NIST publica la versión 1.0 del Marco de Privacidad
  - El NIST ofrece una guía de inicio rápido para su catálogo de salvaguardias de seguridad y privacidad
  - Rincón de la ciberseguridad para la pequeña empresa

- Referencia

Very Good

bitwarden

Departamento de Comercio

Valoración global de Bitwarden: Muy buena

- Recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- El asesoramiento general sobre seguridad está actualizado y cumple las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Comisión Federal de Comunicaciones (FCC)

Hoja de consejos sobre ciberseguridad para pequeñas empresas

- Formar a los empleados en los principios de seguridad. Establezca prácticas y políticas de seguridad básicas para los empleados, como exigir contraseñas seguras y establecer directrices de uso adecuado de Internet, que detallen las sanciones por infringir las políticas de ciberseguridad de la empresa. Establecer normas de comportamiento que describan cómo manejar y proteger la información de los clientes y otros datos vitales.
- Exija a los empleados que utilicen contraseñas únicas y que las cambien cada tres meses. Considere la posibilidad de implantar una autenticación multifactor que requiera información adicional a la contraseña para acceder al sistema. Compruebe con sus proveedores que manejan datos confidenciales, especialmente las instituciones financieras, si ofrecen autenticación multifactor para su cuenta.
- Referencia

10. Passwords and authentication

Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.

Fair

bitwarden

Comisión Federal de Comunicaciones (FCC)

Valoración global de Bitwarden: Regular

- No recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
  - Enlaces a contenidos centrados en la seguridad de las contraseñas
  - Sin embargo, el contenido está claramente desfasado y podría estar mejor organizado.
- No menciona sistemáticamente la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas.
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
  - En contra de las directrices del NIST, recomienda cambiar las contraseñas cada tres meses
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Administración de Pequeñas Empresas (SBA)

Buenas prácticas para prevenir ciberataques

Consejo de la Agencia:

- Los empleados y sus comunicaciones relacionadas con el trabajo son una de las principales causas de filtración de datos en las pequeñas empresas, ya que son vías directas de acceso a sus sistemas. Formar a los empleados en las buenas prácticas básicas de uso de Internet puede ayudar mucho a prevenir los ciberataques.
  - Otros temas de formación que se tratarán son:
    - Detectar mensajes de phishing
    - Utilizar buenas prácticas de navegación por Internet
    - Evitar descargas sospechosas
    - Habilitación de herramientas de autenticación (por ejemplo, contraseñas seguras, autenticación multifactor, etc.)
    - Protección de la información confidencial de proveedores y clientes
- Referencia

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone), and/or something that physically represents the user (fingerprint, facial recognition). Check with your vendors to see if they offer MFA for your various types of accounts (e.g., financial, accounting, payroll).

Good

bitwarden

Administración de Pequeñas Empresas (SBA)

Valoración global de Bitwarden: Buena

- No recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
- Cita la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

Comisión del Mercado de Valores (SEC)

En julio de 2023, la SEC "adoptó normas definitivas que obligarán a las empresas públicas a revelar tanto los incidentes materiales de ciberseguridad que experimenten como, con carácter anual, la información material relativa a su gestión de riesgos de ciberseguridad, estrategia y gobernanza." Dado el papel de la SEC a la hora de imponer el cumplimiento de la ciberseguridad, parece prudente evaluar los propios consejos de la SEC en materia de seguridad de contraseñas.

Una búsqueda de "seguridad de contraseñas" en el sitio web SEC.gov revela 12 documentos, todos los cuales parecen ser de hace años. Hay una página dedicada a la ciberseguridad, pero ofrece recomendaciones bastante generales extraídas de CISA. Una alerta de riesgos de ciberseguridad de 2020 titulada "Ciberseguridad: Safeguarding Client Accounts against Credential Compromise" (Ciberseguridad: Protección de las cuentas de los clientes frente al compromiso de las credenciales) conduce a un PDF en el que se analiza el relleno de credenciales. Aunque la palabra "contraseña" se utiliza en todo el documento, no se menciona explícitamente la "seguridad de la contraseña". Las "contraseñas seguras" se mencionan en el siguiente contexto:

Ciberseguridad: Proteger las cuentas de los clientes contra el compromiso de credenciales

Consejo de la Agencia:

- Mientras las empresas se preparan para los ataques de relleno de credenciales, el personal de OCIE anima a las empresas a considerar sus prácticas actuales (por ejemplo, MFA y otras prácticas descritas anteriormente) y cualquier limitación potencial de esas prácticas, y a considerar si los clientes y el personal de la empresa están debidamente informados sobre cómo pueden proteger mejor sus cuentas. Clientes informados La mayoría de las empresas exigen a sus clientes y empleados que creen y utilicen contraseñas seguras. Sin embargo, el uso de contraseñas es menos eficaz si los clientes y/o el personal reutilizan contraseñas de otros sitios. Para ser más eficaces, algunas empresas han informado y animado a los clientes y al personal a crear contraseñas fuertes y únicas y a cambiarlas si hay indicios de que su contraseña ha sido comprometida.

The Commission has noted that cybersecurity risks have increased alongside the ever-increasing share of economic activity that depends on electronic systems, the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers for information technology services, including cloud computing technology. In my view, artificial intelligence and other technologies may enhance both the ability of public companies to defend against cybersecurity threats but also the capacity of threat actors to launch sophisticated attacks. The Commission also observed that the cost to companies and their investors of cybersecurity incidents is rising at an increasing rate. All of these trends highlight investors' need for improved disclosure.

Fair

bitwarden

Comisión del Mercado de Valores (SEC)

Valoración global de Bitwarden: Regular

- No recomienda el uso de un gestor de contraseñas
- Recuerda la importancia de las contraseñas seguras
  - Enlaces a contenidos antiguos que reconocen las contraseñas seguras, pero que podrían ser mucho más explícitos.
- No menciona sistemáticamente la necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas.
  - Aunque la 2FA/MFA se menciona en el PDF enlazado más arriba, no es un consejo muy extenso y hay que buscar un poco para encontrarlo.
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.

La Casa Blanca

Proclamación del Mes de concienciación sobre la ciberseguridad, 2023

Consejo de la Agencia:

- "Hago un llamamiento a la población, las empresas y las instituciones de Estados Unidos para que reconozcan la importancia de la ciberseguridad y actúen en consecuencia, y para que observen el Mes de la Concienciación sobre la Ciberseguridad en apoyo de nuestra seguridad y resistencia nacionales". También hago un llamamiento a las empresas e instituciones para que tomen medidas que protejan mejor al pueblo estadounidense frente a las ciberamenazas y creen nuevas oportunidades para que los trabajadores estadounidenses puedan optar a ciberempleos bien remunerados. Los estadounidenses también pueden tomar medidas inmediatas para protegerse mejor, como activar la autenticación multifactor, actualizar el software de ordenadores y dispositivos, utilizar contraseñas seguras y ser cautelosos a la hora de hacer clic en enlaces que parezcan sospechosos."

- Referencia

Una experiencia pública digital

Consejo de la Agencia:

- Las agencias se asegurarán de que los sitios web que requieran que el público se autentique sean compatibles con los gestores de contraseñas de uso común, y no impedirán el "pegado" de contraseñas u otros mecanismos de ayuda automatizados del lado del cliente.

- Referencia

Resumen del Simposio de la Casa Blanca sobre modernización de la autenticación multifactor

Consejo de la Agencia:

- "Se necesita algo más que una contraseña para estar seguro en Internet, y ahí es donde entra en juego la autenticación multifactor para garantizar que sus datos estén mejor protegidos frente a ciberdelincuentes malintencionados", afirmó Brandon Wales, Director Ejecutivo de CISA. "CISA ha instado sistemáticamente a las organizaciones a implantar la AMF para todos los usuarios con el fin de garantizar que sea más difícil acceder a cualquier dato crítico. El simposio de hoy consiste en reunirnos para trazar la visión que todos nos esforzamos por hacer realidad".

- Referencia

La Administración Biden-Harris anuncia un programa de etiquetado de ciberseguridad para dispositivos inteligentes con el fin de proteger a los consumidores estadounidenses

Asesoramiento de la Agencia

- Actuando en virtud de su autoridad para regular los dispositivos de comunicación inalámbrica, se espera que la FCC solicite comentarios públicos sobre el despliegue del programa voluntario de etiquetado de ciberseguridad propuesto, que se espera que esté en funcionamiento en 2024. Según lo propuesto, el programa aprovecharía los esfuerzos de las partes interesadas para certificar y etiquetar productos, basándose en criterios específicos de ciberseguridad publicados por el Instituto Nacional de Normas y Tecnología (NIST) que, por ejemplo, exigen contraseñas únicas y fuertes por defecto, protección de datos, actualizaciones de software y capacidades de detección de incidentes.

- Referencia

Good

Updated January 2025

bitwarden

La Casa Blanca

Valoración global de Bitwarden: Buena

- No recomienda el uso de un gestor de contraseñas
  - En un comunicado del Mes de la Concienciación sobre Ciberseguridad de 2022, la Casa Blanca recomendó el uso de un gestor de contraseñas. La Casa Blanca tuvo la oportunidad de hacer lo mismo en el blog 2023 Cybersecurity Awareness. No lo hicieron. Aunque el blog recomienda "utilizar contraseñas seguras", no menciona los gestores de contraseñas.
- Recuerda la importancia de las contraseñas seguras
- Necesidad de 2FA/MFA para reforzar la seguridad de las contraseñas
- Los consejos generales de seguridad no están actualizados y no cumplen las directrices del NIST
  - En comunicaciones anteriores, la Casa Blanca ha recomendado cambiar las contraseñas, en contradicción con el consejo del NIST. Las contraseñas sólo deben cambiarse si son débiles, se han reutilizado o se han visto comprometidas. Puede que nunca sea necesario cambiar una contraseña fuerte y única a menos que sospeches que ha sido comprometida.
- No presenta las recomendaciones de seguridad de las contraseñas de forma clara, comprensible y fácil de encontrar.
  - Sin página dedicada a la ciberseguridad

Resumen

Hay muchas medidas que puedes tomar para mantenerte seguro en Internet, pero la acción más sencilla y con el impacto más significativo e inmediato en tu seguridad es utilizar un gestor de contraseñas. Elija un gestor de contraseñas multiplataforma con cifrado de extremo a extremo de conocimiento cero que pueda generar y almacenar un número ilimitado de contraseñas únicas y seguras. Puedes empezar a utilizar Bitwarden con una cuenta gratuita u optar por Premium por menos de 10 $/año para obtener funciones avanzadas.

Recursos adicionales

- Ver la presentación sobre el estado de la seguridad de las contraseñas